Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Secure Coding Master Course For Banking and Finance

Learn via: **Classroom**

Duration: **5 Day**

Overview

"Money makes the world go round...." – remember? And yes: it is your responsibility to secure all that. As a fintech company you have to take up the challenge, and beat the bad guys with bomb-proof, secure applications!

If there is a domain where security is critical, it is definitely fintech. Vulnerability is not an option if you want to stay a trusted and reliable vendor with systems and applications that certainly comply with PCI-DSS requirements. You need devoted secure coders with high-level professional attitude and developers eager to fight all coding problems: yes, you need a skilled team of software engineers.

Want to know why? Just for the record: even though IT security best practices are widely available, 90% of security incidents stem from common vulnerabilities as a result of ignorance and malpractice. So, you better keep loaded in all possible ways with up to date knowledge about secure coding – unless you *wanna cry*!

We offer a training program exclusively targeting engineers developing applications for the banking and finance sector. Our dedicated trainers share their experience and expertise through hands-on labs, and give real-life case studies from the banking industry – engaging participants in live hacking fun to reveal all consequences of insecure coding.

Prerequisites

There are no prerequisites for this course.

Who Should Attend

Developers working in the banking and finance sector.

What You Will Learn

- Understand basic concepts of security, IT security and secure coding
- Understand security considerations in the SDLC
- Understand special threats in the banking and finance sector
- Understand regulations and standards
- Learn Web vulnerabilities beyond OWASP Top Ten and know how to avoid them
- Learn about XML security
- Learn client-side vulnerabilities and secure coding practices
- Have a practical understanding of cryptography
- Understand the requirements of secure communication
- Understand essential security protocols
- Understand some recent attacks against cryptosystems
- Understand security concepts of Web services
- Learn about JSON security
- Learn about typical coding mistakes and how to avoid them
- Get information about some recent vulnerabilities in the Java framework
- Learn about denial of service attacks and protections
- Get practical knowledge in using security testing techniques and tools
- Learn how to set up and operate the deployment environment securely
- Get sources and further readings on secure coding practices

Outline

- IT security and secure coding

- Special threats in the banking and finance sector
- Regulations and standards
- Web application security (OWASP Top Ten 2017)
- Client-side security
- Security architecture
- Requirements of secure communication
- Practical cryptography
- Crypto libraries and APIs
- Security protocols
- Input validation
- Security of Web services
- Improper use of security features
- Object-relational mapping (ORM) security
- Improper error and exception handling
- Time and state problems
- Code quality problems
- Denial of service
- Security testing techniques and tools
- Deployment environment
- Principles of security and secure coding
- Knowledge sources